Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	22 KB
E-mail Remetente	**Hash da Mensagem**
eliane_mulherviva@mail.com	b72fe7fb3f4bb889d465d1faec321b2c

Data de Envio	Assunto do E-mail	Anexos
03/09/2025 12:57:15	AVISO AO SUPOSTO CREDOR _Possível Fraude e outros	Não contém anexos

Evidências do Destinatário: craraujo@sabesp.com.br

Data/Hora Processamento	Evidência
03/09/2025 12:57:16	Entrega ao Servidor de email iCarta.
03/09/2025 12:57:16	Hash da mensagem iCarta: b72fe7fb3f4bb889d465d1faec321b2c
03/09/2025 12:57:16	Hash da mensagem iCarta do destinatário: 01d7f45e672599f7339ef7cda2084b03 .
03/09/2025 12:57:16	Assinatura DKIM: a=rsa-sha256; b=ZYKddQAuOeWkAU7TQYXPMXG+6oGAMdI1T/HChhDnwBNdnCbnt1hskXwi5YebyaB1LzvAhB/Vfp3YSHd2H0Cjw+bvV5g4SbFO+4o31EYa5Ti87l0prn0e1P9GTXNtPerB5Vq8Z6X3rq3RnhgwwAn4NWNRIRLEZkd1KjdCNFbuDys=; s=dkim; c=relaxed/relaxed; d=icarta.pro; v=1; bh=oA3Zv7cnwcgQtyekvgUmcBF27RB4WUMsbjfGFsuVSEs=; h=From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding; .
03/09/2025 12:57:17	Aposição do Carimbo do Tempo (PLURIO), HLB(Hora Legal Brasileira): 03/09/2025 12:57:17.0 HLB GMT-03:00 destinatário: craraujo@sabesp.com.br
03/09/2025 12:57:17	Processo finalizado para o envio ao destinátario craraujo@sabesp.com.br .
03/09/2025 12:57:22	Início da tentativa de entrega às 2025-09-03 12:57:19 DEBUG: getProvider() returning javax.mail.Provider[TRANSPORT,smtp,com.sun.mail.smtp.SMTPTransport,Oracle] DEBUG SMTP: useEhlo true, useAuth false DEBUG SMTP: trying to connect to host "52.101.10.2", port 25, isSSL false 220 BN1PEPF0000467F.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Wed, 3 Sep 2025 15:57:18 +0000 [08DDE7625FB71E38] DEBUG SMTP: connected to host "52.101.10.2", port: 25 EHLO smtp1.icarta.pro 250-BN1PEPF0000467F.mail.protection.outlook.com Hello [184.73.220.78] 250-SIZE 157286400 250-PIPELINING 250-DSN 250-ENHANCEDSTATUSCODES 250-STARTTLS 250-8BITMIME 250-BINARYMIME 250-CHUNKING 250 SMTPUTF8 DEBUG SMTP: Found extension "SIZE", arg "157286400" DEBUG SMTP: Found extension "PIPELINING", arg "" DEBUG SMTP: Found extension "DSN", arg "" DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg "" DEBUG SMTP: Found extension "STARTTLS", arg "" DEBUG SMTP: Found extension "8BITMIME", arg "" DEBUG SMTP: Found extension "BINARYMIME", arg "" DEBUG SMTP: Found extension "CHUNKING", arg "" DEBUG SMTP: Found extension "SMTPUTF8", arg "" STARTTLS 220 2.0.0 SMTP server ready EHLO smtp1.icarta.pro 250-BN1PEPF0000467F.mail.protection.outlook.com Hello [184.73.220.78] 250-SIZE 157286400 250-PIPELINING 250-DSN

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	22 KB
E-mail Remetente	**Hash da Mensagem**
eliane_mulherviva@mail.com	b72fe7fb3f4bb889d465d1faec321b2c

Data de Envio	Assunto do E-mail	Anexos
03/09/2025 12:57:15	AVISO AO SUPOSTO CREDOR _Possível Fraude e outros	Não contém anexos

250-ENHANCEDSTATUSCODES
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
DEBUG SMTP: Found extension "SIZE", arg "157286400"
DEBUG SMTP: Found extension "PIPELINING", arg ""
DEBUG SMTP: Found extension "DSN", arg ""
DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg ""
DEBUG SMTP: Found extension "8BITMIME", arg ""
DEBUG SMTP: Found extension "BINARYMIME", arg ""
DEBUG SMTP: Found extension "CHUNKING", arg ""
DEBUG SMTP: Found extension "SMTPUTF8", arg ""
DEBUG SMTP: use8bit true
DEBUG SMTP: found an 8bit part
DEBUG SMTP: found an 8bit part
MAIL FROM:<1fa9b7eb-5801-4e6d-8b9e-9caac9f6fcb1-pid@icarta.pro>
250 2.1.0 Sender OK
DEBUG SMTP: sendPartial set
RCPT TO:<craraujo@sabesp.com.br>
250 2.1.5 Recipient OK
DEBUG SMTP: Verified Addresses
DEBUG SMTP: craraujo@sabesp.com.br
DATA
354 Start mail input; end with <CRLF>.<CRLF>
.
250 2.6.0 <3dddda83-f833-4f7a-8c77-173c9adb6653@smtp1.icarta.pro>
[InternalId=43117176732912, Hostname=CPWP152MB6148.LAMP152.PROD.
OUTLOOK.COM] 37269 bytes in 0.474, 76.701 KB/sec Queued mail for delivery
DEBUG SMTP: message successfully delivered to mail server
QUIT
221 2.0.0 Service closing transmission channel

Mensagem entregue às 2025-09-03 12:57:22
.

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	22 KB
E-mail Remetente	**Hash da Mensagem**
eliane_mulherviva@mail.com	b72fe7fb3f4bb889d465d1faec321b2c

Data de Envio	Assunto do E-mail	Anexos
03/09/2025 12:57:15	AVISO AO SUPOSTO CREDOR _Possível Fraude e outros	Não contém anexos

Evidências do Destinatário: danielszlak@hotmail.com

Data/Hora Processamento	Evidência
03/09/2025 12:57:16	Entrega ao Servidor de email iCarta.
03/09/2025 12:57:16	Hash da mensagem iCarta: b72fe7fb3f4bb889d465d1faec321b2c
03/09/2025 12:57:16	Hash da mensagem iCarta do destinatário: 7d7790f291dd0d020afbbecb82c26949 .
03/09/2025 12:57:16	Assinatura DKIM: a=rsa-sha256; b=WeYqT80HanQSZL4DZEltPrJwc5mHyc4MXWMFSs8AFeI3E7CqfLSZM9Aayntn8cXT1K hsvnbP7mulXeqfp8jSvFyQ5bZvgu4mZWTDuqtrZwgNGk7Ijg6VxawDEgLbjwzeVe/rag1y 9DPskEFEW0CEH/ocduD6g9MvRjNu+kg/gK8=; s=dkim; c=relaxed/relaxed; d=icarta.pro; v=1; bh=G9i3OZkaatofXkCHB+mp8f5s12JpdGB6K/+zFOeepl8=; h=From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding; .
03/09/2025 12:57:18	Aposição do Carimbo do Tempo (PLURIO), HLB(Hora Legal Brasileira): 03/09/2025 12:57:18.0 HLB GMT-03:00 destinatário: danielszlak@hotmail.com
03/09/2025 12:57:18	Processo finalizado para o envio ao destinátario danielszlak@hotmail.com .
03/09/2025 12:57:22	Início da tentativa de entrega às 2025-09-03 12:57:19 DEBUG: getProvider() returning javax.mail.Provider[TRANSPORT,smtp,com.sun.mail.smtp.SMTPTransport,Oracle] DEBUG SMTP: useEhlo true, useAuth false DEBUG SMTP: trying to connect to host "52.101.68.20", port 25, isSSL false 220 DU6PEPF0000A7DF.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Wed, 3 Sep 2025 15:57:19 +0000 [08DDEA16433DE684] DEBUG SMTP: connected to host "52.101.68.20", port: 25 EHLO smtp1.icarta.pro 250-DU6PEPF0000A7DF.mail.protection.outlook.com Hello [184.73.220.78] 250-SIZE 49283072 250-PIPELINING 250-DSN 250-ENHANCEDSTATUSCODES 250-STARTTLS 250-8BITMIME 250-BINARYMIME 250-CHUNKING 250 SMTPUTF8 DEBUG SMTP: Found extension "SIZE", arg "49283072" DEBUG SMTP: Found extension "PIPELINING", arg "" DEBUG SMTP: Found extension "DSN", arg "" DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg "" DEBUG SMTP: Found extension "STARTTLS", arg "" DEBUG SMTP: Found extension "8BITMIME", arg "" DEBUG SMTP: Found extension "BINARYMIME", arg "" DEBUG SMTP: Found extension "CHUNKING", arg "" DEBUG SMTP: Found extension "SMTPUTF8", arg "" STARTTLS 220 2.0.0 SMTP server ready EHLO smtp1.icarta.pro 250-DU6PEPF0000A7DF.mail.protection.outlook.com Hello [184.73.220.78] 250-SIZE 49283072 250-PIPELINING 250-DSN

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	22 KB
E-mail Remetente	**Hash da Mensagem**
eliane_mulherviva@mail.com	b72fe7fb3f4bb889d465d1faec321b2c

Data de Envio	Assunto do E-mail	Anexos
03/09/2025 12:57:15	AVISO AO SUPOSTO CREDOR _Possível Fraude e outros	Não contém anexos

250-ENHANCEDSTATUSCODES
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
DEBUG SMTP: Found extension "SIZE", arg "49283072"
DEBUG SMTP: Found extension "PIPELINING", arg ""
DEBUG SMTP: Found extension "DSN", arg ""
DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg ""
DEBUG SMTP: Found extension "8BITMIME", arg ""
DEBUG SMTP: Found extension "BINARYMIME", arg ""
DEBUG SMTP: Found extension "CHUNKING", arg ""
DEBUG SMTP: Found extension "SMTPUTF8", arg ""
DEBUG SMTP: use8bit true
DEBUG SMTP: found an 8bit part
DEBUG SMTP: found an 8bit part
MAIL FROM:<1fa9b7eb-5801-4e6d-8b9e-9caac9f6fcb1-pid@icarta.pro>
250 2.1.0 Sender OK
DEBUG SMTP: sendPartial set
RCPT TO:<danielszlak@hotmail.com>
250 2.1.5 Recipient OK
DEBUG SMTP: Verified Addresses
DEBUG SMTP: danielszlak@hotmail.com
DATA
354 Start mail input; end with <CRLF>.<CRLF>
.
250 2.6.0 <d0fed57d-5596-4973-8334-bc1f7888dd2e@smtp1.icarta.pro>
[InternalId=183094455879393, Hostname=PA4PR05MB7854.eurprd05.prod.
outlook.com] 35556 bytes in 1.040, 33.362 KB/sec Queued mail for delivery -> 250
2.1.5
DEBUG SMTP: message successfully delivered to mail server
QUIT
221 2.0.0 Service closing transmission channel

Mensagem entregue às 2025-09-03 12:57:22
.

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.